Learning Objectives

In this module, we will:

- Identify types of processes and their components
- Identify and explain types and nature of controls
- Describe basic IT concepts including IT application controls, End-User computing controls and IT general controls

Learning Sub-Modules

- Understanding Processes
- Understanding Controls
- Understanding IT Concepts

3

Understanding Processes

In this sub-module, we will:

- Identify types of processes and their components
- Differentiate between policies, procedures and controls

4

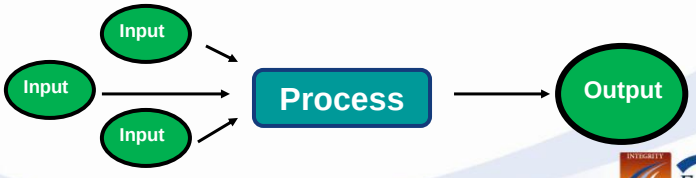
Definitions

Process

- A process is a group of logically related activities that transform inputs into outputs.

Process Owner

- A process owner is a person who is ultimately responsible for the process.



5

Process Inputs, Activities and Outputs

Process Inputs are the material, capital, human resources and information that a business process receives and acts upon in order to transform it into its output.

A **Process Activity** is a specific deed, action or function designed on its own or with other related activities to turn input into output.

Process Outputs are those things transformed by a process for the benefit of the customer or for use as an input in a later process or activity.

See Handout 1

6

Process Boundaries

- The logical beginning and ending of a process
- May be different for each organization
- Impact the documentation of a process
- Boundaries determine:
  - What is included in the process
  - What is excluded from the process
  - The sources of inputs to the process
  - The destination of outputs from the process

7

Understanding a Process – Ask Yourself

- Where does a process begin and end?
  - Consider integration points with other processes
- What are the key activities?
- How is relevant information:
  - Initiated?
  - Authorized?
  - Recorded?
  - Processed?
  - Reported?

8

Process Activities

Classes of transactions are data, information or account detail of a common nature within the financial or other processes of a business.

Transactions are classified as:

- **Routine transactions** - recurring activities performed in the normal course of business.
  - **Example:** Cash disbursements
- **Non-routine transactions** - activities that occur periodically that are not part of the routine flow of transactions.
  - **Example:** Sale of fixed assets
- **Estimation transactions** - activities that involve management assumptions.
  - **Example:** 13th month

9

Handout 2: Understanding Process Components

- Processes
  - Payroll
  - Accounts Payable
  - Accounts Receivable
  - Capital Assets

See Handout 2

10

Policies, Procedures and Controls

Policies detail the principles that guide the actions and decisions in an organization. Policies do not tell "how" to do something, but specify what is acceptable, unacceptable, right and wrong.

Procedures detail the established or prescribed methods to be followed. They describe "how it should be done."

Controls are any action taken to mitigate or manage risk and increase the probability that the organization/process will achieve its goals and objectives.

Summary

In this sub-module, we:

- Identified types of processes and their components
- Differentiated between policies, procedures and controls

Understanding Controls

In this sub-module, we will:

- Identify and explain types of controls
- Identify and explain the nature of controls
- Introduce the concept of Entity-Level controls

Controls – Definition

A **control** is defined as any action taken to mitigate or manage risk and increase the probability that the organization/process will achieve its goals and objectives.

What Should We Know About Controls?

- Controls help organizations achieve objectives by mitigating risks.
- The significance of a control relates back to the significance of the risk it is mitigating.
- Risks may be over or under controlled (cost vs. benefit).
- One control may mitigate multiple risks.
- Multiple controls may be required to mitigate one risk.

Types of Controls - Prevent

- **Prevent Controls –** controls used by management to prevent errors from occurring, i.e., stop something from going wrong:
  - Authorization of payments prior to processing
  - Customer credit limit checks
  - Restricting user access to IT systems

Types of Controls - Detect

- **Detect Controls** - control activities that are designed to detect and correct in a timely manner an error or irregularity that would materially affect the achievement of the organization's objectives.
  - Identify when something has gone wrong and correct it:
    - General ledger reconciliations
    - Review of exception reports
    - Quarterly review of system access

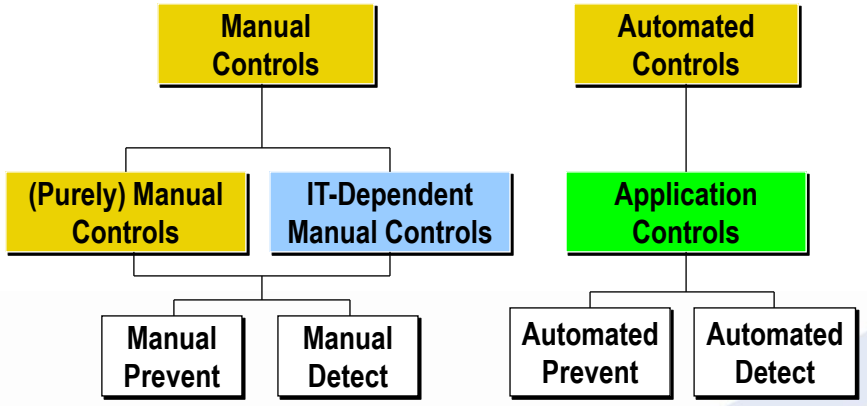
17

Nature of Controls

- Manual Control:
  - Independent review of general ledger reconciliations
  - Authorization of employee expense reports
- IT-dependent manual controls are specific process controls that are manually performed, but require input based upon the results of computer-produced information
  - Review and follow-up of exceptions on a payroll exception report
- IT Application Control:
  - Automated three-way match
  - Data input validation checks
    - For example, customer orders can only be processed using a valid customer number.
  - Restricted user access

18

Classification of Controls



19

Frequency of Controls

- Examples of how often controls are performed
  - Ongoing
    - Firewall
  - Daily/Multiple times per day
    - Purchase order approval
  - Monthly
    - Review of general ledger reconciliations
  - Quarterly
    - Review of user access to IT systems
  - Annually
    - Physical Inventory
  - Ad hoc/As required
    - Authorization of termination payment to employees

20

Control Owner

Understanding who owns the control helps determine:

- If the control is designed effectively
  - Is the person performing the control appropriate?
    - For example, general ledger reconciliations are performed by the accountant rather than the goods receiving clerk.
- Whether there is appropriate segregation of duties
  - Is the same person responsible for the initiation, authorization and recording of transactions?
- Whom to contact to understand and test the control

21

Control Identification

- Identify what may prevent or detect an error or minimize its impact.
- Ask yourself:
  - Does the control mitigate the risk?
  - Does the related risk require a combination of controls?
    - If yes:
      - What is the most effective and efficient combination?
  - Are additional controls required to adequately mitigate the related risk?

22

Entity-Level Controls

- Entity-level controls set the tone and establish the expectations of the organization's control environment, often referred to as "tone at the top".
  - Indirect: cross-functional and affect the achievement of the entity's control objectives in indirect, but important ways
    - Examples: hiring practices, training efforts, tone at the top, code of conduct or code of ethics
  - Direct: designed to have a specific and direct effect on the control objectives related to financial reporting elements
    - Examples: monthly reviews of operational results which measure performance and analytics (e.g., variance analysis)

EAGLE North Carolina Office of the State Controller

Summary

In this sub-module, we:

- Identified and explained types of controls
- Identified and explained the nature of controls
- Introduced the concept of Entity-Level controls

EAGLE North Carolina Office of the State Controller

Understanding IT Concepts

In this sub-module, we will:

- Describe basic IT concepts
  - Describe IT Application Controls
  - Describe End-User Computing Controls
  - Describe IT General Controls
- Explain relation to overall IT Environment

25

Why Do We Need to Understand IT?

- Most processes that we examine use IT systems.
- When evaluating how well risk is managed within a process, an understanding of the IT environment and IT controls is necessary to develop test plans accordingly.

See Handout 3

26

Application Controls

Application controls are:

- System settings, based on the organization's business rules, that determine how transactions and data will be input to, processed by, and included in the output of the computer system
- Standard application functionality or custom-developed
- Often called configuration controls

27

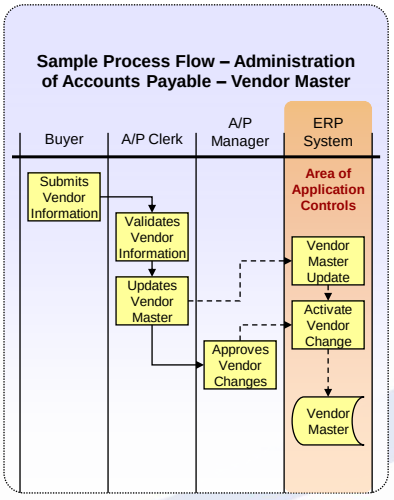
Application Controls – Components

- We are concerned with the following components of application controls:
  - Configuration settings and custom automated controls
  - Master data controls and access
  - Control overrides
  - Segregation of duties and function access
  - Interface controls

28

Examples of Application Controls

- Data entry/field validations (for example, validation of entered credit card numbers)
- Workflow rules (for example, electronic routing and sign-off of purchase requests)
- Field entries being enforced based on predefined values (for example, pricing information)
- Work steps being enforced based on pre-defined status transitions (for example, open > reviewed > closed)
- Automated calculations



End-User Computing Controls

- End-User Computing generally involves the use of end-user developed spreadsheets and databases.
- It is pertinent to ensure adequate controls are in place for those high risk spreadsheets, databases and other user-developed programs as they are equivalent to any other system.
- Example End-User controls:
  - Access control
  - Version/change control
  - Reviewed for completeness, accuracy and processing integrity
  - Backup

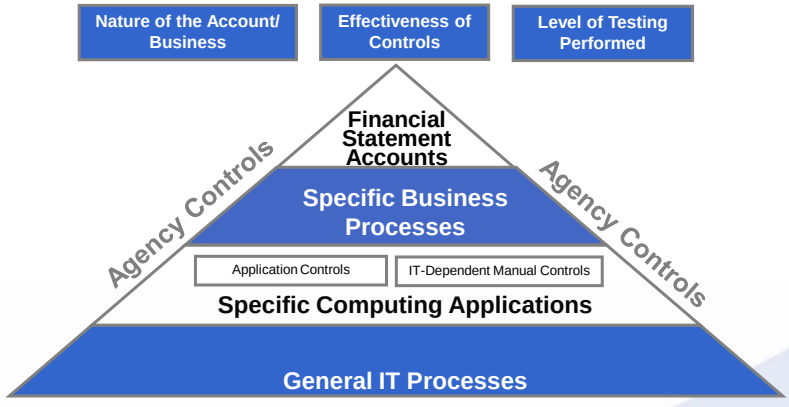
IT General Controls

- IT General Controls are controls over:
  - System software acquisition and maintenance
  - Access security
  - Computer operations
  - Application system acquisition, development and maintenance
- IT general controls are the foundation for application controls
- IT general controls affect IT-dependent manual controls

See Handout 4

31

The IT Environment



32

Summary

In this sub-module, we:

- Described the basic IT concepts
  - Described IT Application controls
  - Described End-User Computing Controls
  - Described IT General Controls
- Explained relation to overall IT Environment

33

Module Summary

In this module, we:

- Identified types of processes and their components
- Identified and explained types and nature of controls
- Described basic IT concepts including IT application controls, End-User computing controls and IT general controls

34

Appendix

How to Document a Control on Narrative or Flowchart

When documenting a control, the following should be considered:

- Who performs the control activity (title)
- What is the control activity (not the process)
- When is the control activity performed
- Why is the control activity performed
- How is the control activity documented

A control description should be written such that the testing of the control is readily apparent.

Control – Good and Bad Examples

A bad example of a control description is as follows:

"**He or she** reconciles the goods receipt note and purchase order to the invoice."

A good example of a control description is as follows:

"**The Accounts Payable supervisor** reconciles the goods receipt note and purchase order to the invoice to ensure what is actually paid agrees."

37

Control – Good and Bad Examples (Cont.)

A bad example of a control description is as follows:

"Jane reviews the reconciliation."

A good example of a control description is as follows:

"**The Accounts Payable supervisor** reviews the accounts payable reconciliation for evidence of approval on a monthly basis and also reviews supporting evidence for a sample of reconciling items."

38

Recap Summary

- Module 4:
  - We discussed the theory of, and how to perform, Financial Statement Risk Assessments.
- Module 5:
  - We discussed and identified types of processes and controls.
  - We described basic IT concepts and explained the relation of IT application controls, End-User computing controls and IT general controls to the overall IT environment